National Infrastructure Advisory Council (NIAC)

Intelligence Coordination Working Group

John T. Chambers
President and CEO
Cisco Systems, Inc.

Gilbert G. Gallegos
Retired Chief of Police
Albuquerque, NM

Overview

- Purpose
- Actions Taken
- Guiding Principle
- Context
- Findings
- Case Studies
- CEO Survey
- Conclusions

Purpose

- Improve coordination between critical infrastructure sectors and the Intelligence Community to protect critical infrastructures

Actions Taken

- Formed Study Group
- Held four workshops and bi-weekly calls
- Defined and studied key issues
- Used recent events as case studies
- Interviewed CEOs and IC seniors for executive perspective

Guiding Principle

- Critical infrastructure sectors differ greatly in terms of
  - Needs
  - Complexity
  - Regulatory environments
  - National boundaries
  - Organization
- "One size fits all" solutions will not suffice
- Recommendations aim to improve national capability, but allow for sector differences
  - Architecture approach
  - Process-based trust relationships
  - Information protection

Context

- Findings and recommendations must be applied to:
  - Deterrence
  - Protection
  - Preparedness
  - Crisis Management and Response
  - Recovery (Restoration and Reconstitution)
- Implementation will depend on level of focus
  - Strategic planning and decision-making
  - Operational or tactical decision-making

Findings

- Differences in experience, vocabulary, culture, and specialized skills inhibit information exchange and analysis
- Current information sharing mechanisms complex, poorly understood, not customer focused
- Government caveats and classifications impede timely and appropriate information sharing
- Current alert and warning process does not reach appropriate decision makers

Case Studies

- Purpose: Illustrate issues and findings
- Four recent significant incidents involving critical infrastructures and the intelligence community
  - Focused on information sharing
  - Covered all hazards to critical infrastructures
  - Two cases represent pre-event warnings to critical infrastructures
  - Two cases represent post-event analysis
  - Three cases related to terrorist acts or intentions; the other was a non-hostile event
    - August 2003 Blackout
    - July 2004 Financial Services Threat Alert
    - July 2005 London Bombings
    - October 2005 New York Public Transit Threat Alert

CEO Survey

- Survey questions related to changes since 9/11/2001:
  - Investment strategies
  - Training priorities
  - Information requirements (from government)
  - Information sharing (with government)
  - Top-level concerns
  - Board involvement
- Survey concerned with information sharing necessary to support CEO policy and investment decisions
- Could provide useful guidance to upcoming DNI strategic planning effort

Common CEO Themes

- Implications of 9/11 considered and incorporated without strategic input from government
- Claims of inadequate security not supported by shared intel or criteria but worst-case speculation
- Inability to provide meaningful information for policy and investment decisions due to:
  - Absence of agreement on end-state
  - No joint processes for planning and implementation
  - Lack of understanding of sector business operations
- More emphasis placed on response than additional protection w/o credible threat information

Preliminary Recommendations

- Establish trusted CEO-IC relationships
- Create process for CEO-IC strategic planning and information sharing
- Develop sector business expertise in IC to better identify and satisfy information needs; establish liaisons with relevant corporate officers
- Focus on information requirements not classification

Conclusions

- All involved in Critical Infrastructure Protection doing the best they can with information they have
- Better information sharing will improve timely actions and coordination
- Recommendations simple, but not easy

Questions and Answers